Discrete Mathematics 79 (1989/90) 229–234
North-Holland

SOME REMARKS ON NUMBER OF PARAMETERS OF THE SOLUTIONS OF BOOLEAN EQUATIONS

Dragić BANKOVIĆ
Department of Mathematics, University Kragujevac, Yugoslavia

Received 14 January 1986
Revised 4 November 1987

The parametric solution of Boolean equations in n unknowns is defined as the system $\phi = (\gamma_1, \ldots, \gamma_n)$ of Boolean functions $\gamma_1, \ldots, \gamma_n : B^n \to B$, i.e. the parametric solution is defined by $x_i = \gamma_i(t_1, \ldots, t_n)$ $(i = 1, \ldots, n)$. In this paper we show that the functions $\gamma_i (i = 1, \ldots, n)$ depend on less than n parameters. The speciale case is $x_i = \gamma_i(t_1, \ldots, t_i)$ $(i = 1, \ldots, n)$ which can be obtained by the method of successive eliminations.

Let $X = (x_1, \ldots, x_n) \in B^n$, $T = (t_1, \ldots, t_n) \in B^n$ and $A = (a_1, \ldots, a_n) \in \{0, 1\}^n$, where $(B, \cup, \cdot, ', 0, 1)$ is Boolean algebra.

Definition. Let $f : B^n \to B$ be a Boolean function. The system $\psi = (\psi_1, \ldots, \psi_n)$ of Boolean functions $\psi_1, \ldots, \psi_n : B^n \to B$ is the general solution of consistent equation $f(X) = 0$ if and only if

$$(\forall x) f(\psi(X)) = 0 \wedge (\forall X)(f(X) = 0 \Rightarrow (\exists T)(X = \psi(T))).$$

Theorem 1 (Löwenheim). *Let $f : B^n \to B$ be a Boolean function. Then*

$$(\forall X) f(X) = 0 \Leftrightarrow (\forall A \in \{0, 1\}^n) f(A) = 0$$

See, for instance, [2].

Theorem 2 (Deschamps). *Let $f : B^n \to B$ be a Boolean function and assume that equation $f(X) = 0$ is consistent. The formulas $X = \phi(T)$, where $\phi = (\gamma_1, \ldots, \gamma_n)$ and $\gamma_i : B^n \to B$ $(i = 1, \ldots, n)$, define the general solution of equation $f(X) = 0$ if and only if*

$$(\forall X)\left(f(X) = \prod_A \bigcup_{i=1}^{n} (\gamma_i(A) + x_i)\right),$$

where $\prod_A$ means the product over all $A = (a_1, \ldots, a_n) \in \{0, 1\}^n$ and operation $+$ is defined as $a + b = a'b \cup ab'$.

See [1].

Lemma 1. *Let* $f: B^n \to B$ *and* $\gamma_i: B^n \to B$ $(i = 1, \ldots, n)$ *be simple Boolean functions and* $\phi = (\gamma_1, \ldots, \gamma_n)$. *Let us assume that equation* $f(X) = 0$ *is consistent.* $X = \phi(T)$ *is the general solution of equation* $f(X) = 0$ *in Boolean algebra* B *if and only if* $X = \phi(T)$ *is the general solution of equation* $f(X) = 0$ *in two-element Boolean algebra* B_2.

Proof. "$X = \phi(T)$ is the general solution of equation $f(X) = 0$ in B".

$$\Leftrightarrow (\forall X)\left(f(X) = \prod_C \bigcup_{i=1}^{n} (\gamma_i(C) + x_i)\right)$$

(by Theorem 2)

$$\Leftrightarrow (\forall X)\left(f(X) + \prod_C \bigcup_{i=1}^{n} (\gamma_i(C) + x_i) = 0\right)$$

$$\Leftrightarrow (\forall A \in \{0, 1\}^n)\left(f(A) + \prod_C \bigcup_{i=1}^{n} (\gamma_i(C) + a_i) = 0\right)$$

(by Theorem 1)

$$\Leftrightarrow (\forall A \in \{0, 1\}^n)\left(f(A) = \prod_C \bigcup_{i=1}^{n} (\gamma_i(C) + a_i)\right)$$

$\Leftrightarrow$ "$X = \phi(T)$ is the general solution of equation $f(X) = 0$ in B_2" (by Theorem 2). □

Theorem 3. *Let* $f: B^n \to B$ *be a simple Boolean function. The general solution of Boolean equation* $f(X) = 0$ *can be written in the form*

$$\begin{aligned} x_1 &= h_1(t_1, \ldots, t_{n-m}) \\ &\vdots \\ x_n &= h_n(t_1, \ldots, t_{n-m}) \end{aligned} \tag{1}$$

where $h_i: B^n \to B$ $(i = 1, \ldots, n)$, *if and only if*

$$\prod_A f(A) = 0 \wedge \bigcup_S \prod_{A \notin S} f(A) = 1, \tag{2}$$

where $S \subset \{0, 1\}^n$ *and* $\operatorname{card} S = 2^{n-m}$ ($\operatorname{card} S$ *is the cardinal number of the set* S).

Proof. Using the notation $h = (h_1, \ldots, h_n)$, we can write (1) in the form $X = h(T)$. $X = h(T)$ is the general solution in B if and only if it is the general solution in B_2, by Lemma 1. We shall prove that formulas (1) define the general solution in B_2 if and only if number r of the particular solutions of equation $f(X) = 0$ in B_2 satisfies $1 \leqslant r \leqslant 2^{n-m}$. Let $1 \leqslant r \leqslant 2^{n-m}$. We can make the following

table:

t_1	t_2	...	t_{n-m}	x_1	...	x_n
0	0		0			
0	0		1			
⋮	⋮		⋮			
1	1		1			

The table has 2^{n-m} rows because $(t_1, \ldots, t_{n-m}) \in \{0, 1\}^{n-m}$. In the columns for $x_1, \ldots, x_n$ we write all particular solutions of $f(X) = 0$.

If $r = 2^{n-m}$ then the table is complete. If $r < 2^{n-m}$ then we complete the rest of the table with arbitrary particular solutions of equation $f(X) = 0$. From the table we get

$$x_1 = h_1(t_1, \ldots, t_n)$$
$$\vdots$$
$$x_n = h_n(t_1, \ldots, t_n),$$

where $h_1, \ldots, h_n$ are the canonical disjunctive forms for $x_1, \ldots, x_n$, respectively, obtained from the table.

Let (1) define the general solution of equation $f(X) = 0$. Using (1) we can get at most 2^{n-m} different n-tuples $(x_1, \ldots, x_n)$ when $(t_1, \ldots, t_{n-m}) \in \{0, 1\}^{n-m}$. Since equation $f(X) = 0$ is consistent we have $1 \leqslant r \leqslant 2^{n-m}$.

We can remark the following: formula (2) holds if and only if number r of the particular solutions of equation $f(X) = 0$ in B_2 satisfies $1 \leqslant r \leqslant 2^{n-m}$.

Thus we have

"$X = h(T)$ is the general solution of $f(X) = 0$ in B"

$\Leftrightarrow$ "$X = h(T)$ is the general solution of $f(X) = 0$ in B_2"

$\Leftrightarrow$ "number r of the particular solutions of equation $f(X) = 0$ in B_2 satisfies $1 \leqslant r \leqslant 2^{n-m}$"

$\Leftrightarrow$ (2),

The theorem is proved. □

Corollary 1 [2]. *Let $f : B^n \to B$ be a simple Boolean function. Equation $f(X) = 0$ has a unique solution if and only if*

$$\prod_A f(A) = 0 \wedge \bigcup_A \prod_{C \neq A} f(C) = 1. \tag{3}$$

Proof. Putting in Theorem 3 $m = n$ the conjunction (2) becomes (3) and $h_i (i = 1, \ldots, n)$ are constants. □

Theorem 4. *Let $f: B^n \to B$ be a simple Boolean function. The general solution of equation $f(X) = 0$ is of the form*

$$\begin{aligned}
&x_{j_1} = t_{j_1}\\
&\vdots\\
&x_{j_m} = t_{j_m}\\
&x_{i_1} = g_{i_1}(t_{j_1}, \ldots, t_{j_m}, t_{i_1})\\
&x_{i_2} = g_{i_2}(t_{j_1}, \ldots, t_{j_m}, t_{i_1}, t_{i_2})\\
&\vdots\\
&x_{i_p} = g_{i_p}(t_{j_1}, \ldots, t_{j_m}, t_{i_1}, t_{i_2}, \ldots, t_{i_p})
\end{aligned} \tag{4}$$

$(m, p \in \{1, \ldots, n\}$, $m + p = n$ and $g_{i_v}: B^{m+v} \to B$ $(v = 1, \ldots, p))$ if and only if

$$\bigcup_{A_m} \prod_{A_p} f(a_1, \ldots, a_n) = 0 \tag{5}$$

where $A_m = (a_{j_1}, \ldots, a_{j_m}) \in \{0, 1\}^m$, $A_p = (a_{i_1}, \ldots, a_{i_p}) \in \{0, 1\}^p$ and $\{j_1, \ldots, j_m, i_1, \ldots, i_p\} = \{1, \ldots, n\}$.

Proof. Let us write the formulas (4) as $X = G(T)$. $X = G(T)$ is the general solution in B if and only if $X = G(T)$ is the general solution in B_2, by Lemma 1. Thus it is sufficient to prove that the formulas (4) define the general solution of equation $f(X) = 0$ in B_2 if and only if (7) holds.

We introduce the following notation:

$$f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{i_p})) = f(t_1, \ldots, t_n).$$

Let (5) hold. The condition (5) means, in B_2, that for every m-tuple $(a_{j_1}, \ldots, a_{j_m}) \in \{0, 1\}^m$ there exists a p-tuple

$$(a_{i_1}, \ldots, a_{i_p}) \in \{0, 1\}^p \text{ such that } f((a_{j_1}, \ldots, a_{j_m}), (a_{i_1}, \ldots, a_{i_p})) = 0.$$

We make the following table:

t_{j_1}		t_{j_m}	t_{i_1}		t_{i_p}	x_{j_1}	...	x_{j_m}	x_{i_1}	...	x_{i_p}
0	...	0	0	...	0						
0	...	0	0	...	1						
⋮		⋮	⋮		⋮						
1	...	1	1	...	1						

The table has 2^n rows because $(t_{j_1}, \ldots, t_{j_m}, t_{i_1}, \ldots, t_{i_p}) \in \{0, 1\}^n$. For $(t_{j_1}, \ldots, t_{j_m}, t_{i_1}, \ldots, t_{i_p}) \in \{0, 1\}^n$ we determine $(x_{j_1}, \ldots, x_{j_m}, x_{i_1}, \ldots, x_{i_p}) \in \{0, 1\}^n$ in the

following way:

1. If $f((t_{j_1}, \ldots, t_{jm}), (t_{i_1}, \ldots, t_{i_p})) = 0$ then
   $x_{j_1} = t_{j_1}, \ldots, x_{j_m} = t_{j_m}$,
   $x_{i_1} = t_{i_1}, \ldots, x_{i_p} = t_{i_p}$.

2.1. If $f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{ip})) = 1$ and
$f((t_{j_1}, \ldots, t_{j_m}), (t_{i_n}, \ldots, t'_{ip})) = 0$ then
$x_{j_1} = t_{j_1}, \ldots, x_{j_m} = t_{j_m}$,
$x_{i_1} = t_{i_1}, \ldots, x_{i_{p-1}} = t_{i_{p-1}}, x_{i_p} = t'_{i_p}$.

2.2. If $\Pi_{A_{p-k}} f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{i_{k-1}}, t_{i_k}, a_{k+1}, \ldots, a_p)) = 1$ and $\Pi_{A_{p-k}} f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{i_{k-1}}, t'_{i_k}, a_{k+1}, \ldots, a_p)) = 0$ for some $k \in \{1, \ldots, p\}$ (there exists such k and it is unique, by the condition (5)) then

$$x_{j_1} = t_{i_1}, \ldots, x_{j_m} = t_{j_m}$$
$$x_{i_1} = t_{i_1}, \ldots, x_{i_{k-1}} = t_{i_{k-1}}, x_{i_k} = t'_{i_k},$$
$$x_{i_{k+1}} = e_{k+1}, \ldots, x_{i_p} = e_p$$

where $e_{k+1} \ldots e_p$ is the minimal number, in the binary expansion, of the set

$$\{a_{k+1} \ldots a_p \mid (a_{k+1}, \ldots, a_p) \in \{0, 1\}^{p-k} \wedge f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{i_k}, a_{k+1}, \ldots, a_p)) = 0\}.$$

Let us prove that x_{i_r} $(r = 1, \ldots, p)$ depends only on $t_{j_1}, \ldots, t_{j_m}, t_{i_1}, \ldots, t_{i_r}$. Let $(t_{j_1}, \ldots, t_{j_m}, t_{i_1}, \ldots, t_{i_r}) \in \{0, 1\}^{m+r}$. If $\Pi_{A_{p-r}} f((t_{j_1}, \ldots, t_{j_m}), (t_{i_\perp}, \ldots, t_{i_r}, a_{r+1}, \ldots, a_p)) = 0$ then

$$x_{j_1} = t_{j_1}, \ldots, x_{j_m} = t_{j_m}, x_{i_1} = t_{i_1}, \ldots, x_{i_r} = t_{i_r}$$

for all $(t_{i_{r+1}}, \ldots, t_{i_p}) \in \{0, 1\}^n$ by this procedure. If $\Pi_{A_{p-s}} f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{i_s}, a_{s+1}, \ldots, a_p)) = 1$ $(s < r)$ and $\Pi_{p-s} f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t'_{i_s}, a_{s+1}, \ldots, a_p)) = 0$ then, by this procedure, for all $(t_{i_{s+1}}, \ldots, t_{i_p}) \in \{0, 1\}^{p-s}$ (which means also for all $(t_{i_{r+1}}, \ldots, t_{i_p}) \in \{0, 1\}^{p-r}$) we have

$$x_{j_1} = t_{j_1}, \ldots, x_{j_m} = t_{j_m}, x_{i_1} = t_{i_1}, \ldots, x_{i_s} = t'_{i_s},$$
$$x_{i_{s+1}} = c_{s+1}, \ldots, x_{i_p} = c_p,$$

where $c_{s+1} \ldots c_p$ is the minimal number, in the binary expansion, of the set $\{d_{s+1}, \ldots, d_p \mid (d_{s+1}, \ldots, d_p) \in \{0, 1\}^{p-s} \wedge f((t_{j_1}, \ldots, t_{j_m}), (t_{i_1}, \ldots, t_{i_s}, d_{s+1}, \ldots, d_p)) = 0\}$. We conclude that x_{i_r} does not depend on $(t_{i_{r+1}}, \ldots, t_{i_p})$.

If we write the canonical disjunctive form for $x_{j_1}, \ldots, x_{j_m}, x_{i_1}, \ldots, x_{i_p}$ from the table, we get (4).

Let (4) define the general solution of equation $f(X) = 0$ in B_2. Let $(b_1, \ldots, b_m)$ be an arbitrary element of the set $\{0, 1\}^m$ and let $(d_1, \ldots, d_p)$ be an arbitrary element of the set $\{0, 1\}^p$. If we take

$$t_{j_1} = b_1, \ldots, t_{j_m} = b_m, t_{i_1} = d_1, \ldots, t_{i_p} = d_p,$$

we get, by (4),

$$x_{j_1} = b_1$$
$$\vdots$$
$$x_{j_m} = b_m$$
$$x_{i_1} = g_{i_1}(b_1, \ldots, b_m, d_1) = \alpha_1$$
$$\vdots$$
$$x_{i_p} = g_{i_p}(b_1, \ldots, b_m, d_1, \ldots, d_p) = \alpha_p.$$

Since $f((b_1, \ldots, b_m), (\alpha_{i_1}, \ldots, \alpha_p)) = 0$, then

$$\prod_{A_p} f((b_1, \ldots, b_m), (a_{i_1}, \ldots, a_{i_p})) = 0, \tag{6}$$

where $\prod_{A_p}$ means the product over all $A_p = (a_{i_1}, \ldots, a_{i_p}) \in \{0, 1\}^p$. Because (6) holds for arbitrary $(b_1, \ldots, b_m) \in \{0, 1\}^m$ we have

$$\bigcup_{A_m} \prod_{A_p} f((a_{j_1}, \ldots, a_{j_m}), (a_{i_1}, \ldots, a_{i_m})) = 0$$

where $\bigcup_{A_m}$ means the union over all $A_m = (a_{j_1}, \ldots, a_{j_m}) \in \{0, 1\}^m$. □

Putting $p = n$ in Theorem 4 we get

Corollary 2. *Let $f: B^n \to B$ be a simple Boolean function. If $\prod_A f(A) = 0$ then the general solution of equation $f(X) = 0$ is of the form*

$$x_1 = q_1(t_1)$$
$$x_2 = q_2(t_1, t_2)$$
$$\vdots$$
$$x_n = q_n(t_1, t_2, \ldots, t_n)$$

where $q_i: B^i \to B$ $(i = 1, \ldots, n)$ are simple Boolean functions.

Remark. The last "triangular" form can be obtained, for example, by the method of successive eliminations.

References

[1] J.P. Deschamps, Parametric solutions of Boolean equations, Discrete Mathematics 3 (1972) 333–342.

[2] S. Rudeanu, Boolean Functions and Equations (North-Holland, Amsterdam–London and Elsevier, New York, 1974).